SAFETY ISSUES

R. ROHAL
NASA Lewis Research Center

One of the primary safety issues is that we have three organizations involved, NASA, DOD and DOE. These organizations have three sets of safety requirements that address and possibly overlap various aspects of the systems we are currently talking about. We have review processes that address each one, so I think that the significant issue is that we have to have some way or another to mold these requirements, as well as the review process, together. If we don't do this, it is going to become cumbersome and may crimp the program. I think that we within NASA are already experiencing this somewhat with regards to Space Station.

We have decided on just what the safety requirements will be for Space Station. However, these requirements are not in one single spot so that the designer can go to them and very easily find out what he has to do to be safe. As of this time, we really have not even defined a safety review process as far as Space Station is concerned.

I think that we may be able to get by for a long time on the Space Station in this current environment, but as time goes on it's going to become more and more difficult, especially for something that has a lot more public visibility such as a sizeable nuclear power source in space. This certainly will be questioned much earlier than something like Space Station. Now I would like to talk about the NASA safety review process.

The purpose of the NASA safety review process is to make sure that we preclude, as early as possible, any system hazards that can endanger the manned flight system. Today, I am going to be talking about the systems that address manned flight in a payload safety review process. However, the philosophy behind it really is NASA's philosophy in addressing how we want to treat safety with systems that interact with man. Payloads that interact with man are definitely handled this way. The shuttle system itself, the orbiter and its elements are handled in a very similar fashion.

The intent is to protect the public, its property, the environment and of course the flight hardware as well as the men associated with it. The responsibility clearly lies with the line management. It's the responsibility of the engineer to design a safe vehicle. It isn't, however, always clear what constitutes "safe." We need to clearly state what the requirements are so that the designers and engineers understand them.

Finally, I think the safety organization itself is responsible for review oversight, independent assessment, and defining and making sure that the requirements are disseminated and understood.

The types of basic hazards that we normally address on any of the payloads are:

contamination, electrical shock, explosion, radiation, and temperature extremes. With regard to any one of these particular items, there are a lot of documents which define very specifically what materials you can and can't use, what safety factors you should design and etc.. Of course, all of the hazards are appropriately documented, and either periodically reviewed, or approved both by the safety organization and the program management.

The critical thing is the way NASA defines the severity of the hazard. And as far as NASA is concerned, your design must be dual failure tolerant, you have a critical hazard that will cause a damage or failure of some space hardware or injury to personnel.

With regard to their systems that interface with man, NASA really requires designs that are dual failure tolerant. It's difficult to get around this, and is something that should be considered in our talk today. This became stronger with regards to Space Station and shuttle since the Challenger event.

The primary document that NASA uses, as far as its manned programs are concerned, is a hazard report. Essentially this report identifies the hazard, tells you what causes the hazard, tells you how to control the hazard, and tells you how you are going to verify through analysis and testing. I really stress testing because on the manned systems, you really have to have some tests supporting your claims, and your analysis on critical and catastrophic hazards. Then of course you have the appropriate approvals.

This is just the surface of what goes into a hazard report. A hazard report could be several hundred pages long. It tells the review committees how you are going to eliminate the particular hazard.

Safety analysis is just part of the verification process, and probably less important than the two system analysis or the system test. There are analyses that are accepted and address the various systems. Normally we have fault trees, FMEA's, and various calculations to show that the systems are indeed safe and reach their margins of safety.

The review process is conducted in several phases. We have an initial review and a conceptual state, (the project more or less presents the concept). They identify the operations, both from the ground standpoint and from the flight standpoint. The safety organization is there to help interpret and help the project to prepare for the Phase 0.

Phase 1 comes around right after the Preliminary Design Review. Here you start to clearly define all the hazards, and you produce your preliminary hazard report, your approach to verification, etc.

The Phase 2 review is conducted right after your critical design review. Here you have considerably more material to present, such as engineering drawings, and most analyses. You more or less define how you are going to control your hazards.

Phase 3 is the most critical. It occurs after you have done most of your testing and qualification. Here you really understand how your system is going to work, you understand the problems that your system has had, and you are able to show that you have tested and qualified the equipment to the environments that you expect to see in a particular application.

The DOE process and the DOD process are somewhat similar, but they are different. In the nuclear world, independent reviews are scheduled periodically.

In the Space Station world there is a process defined, (it's awaiting final cost approval from Dick Lures, the program director), but that process is very similar to this used by shuttle. The payload process that Bob is pointing out is a part of shuttle process. The review that he is describing, the ones that Space Station will have, are not done by direct program people. When they are reviewed, the information is provided by those in the program. The hazard reports are developed, the hazard analyses are done and then they are reviewed by people not directly involved in the program, but who do have sufficient knowledge to perform the review.

That information then gets forwarded through the independent safety and product assurance organization, up to the program director for his final concurrence or rejection. That process is in effect an independent review. They use separate engineering people, separate propulsion and electrical folks to review the work that has been done by the program engineering people.

For this particular process, a lot of the technical review is done indepedently of the program by people at Johnson. In the case of the Space Station I am not sure we defined exactly who the independent technical reviewers will be. We have not gone this far yet, have we?

I guess my final word is that I think the primary safety issue is that we really don't have a set of requirements defined for space nuclear plants that we can easily locate. I am not saying that we ought to go out and redefine requirements, but I think we need to provide some sort of a road map as to which requirements exist and where. If there are conflicts, what should we do about those conflicts? Secondly I think that we need to consider just what the review process shall be.

It's going to be pretty difficult for the designers to design easily with safety in mind if we don't do this for them. They are going to have a difficult time really understanding what the requirements are, so my recommendation is that we get the safety communities of NASA, DOE and DOD together and jointly define just what the requirements are, how to get to all the requirements, and also start to define just how we are going to do the appraisal, and evaluation of the designs and the resulting data.

I think that there are good safety organizations in all three of those organizations. I think that we have to get them together. We have to be able to identify what are the right things

to do, what to do about those surface conflicts and then get them resolved. Finally, we need to set forth just how we are going to show the public that we have made sure that we have safety systems.